UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION
3:24-cv-00142-MOC-SCR

BRIAN CAPIAU, on behalf of himself and all others similarly situated,	)	
Plaintiff,	)	
vs.	)	**ORDER**
ASCENDUM MACHINERY, INC.,	)	
Defendant.	)	

THIS MATTER comes before the Court on Defendant's motion to dismiss. (Doc. No. 15). Plaintiff responded in opposition and Defendant filed a reply. (Doc. Nos. 20, 21). This matter is now ripe for disposition.

I. Background

a. Factual Background

Plaintiff Brian Capiau ("Capiau") worked for Defendant Ascendum Machinery, Inc. ("Ascendum") from May 2023 to January 2024. Ascendum, a construction equipment dealer headquartered in North Carolina, maintains computer systems containing the personally identifiable information ("PII") of current and former employees, and employees' minor children. Ascendum's Privacy Policy stipulates that "[Ascendum] strive[s] to use commercially acceptable means to protect [y]our [p]ersonal [d]ata" and that Ascendum "will take all steps reasonably necessary to ensure that [y]our data is treated securely and . . . no transfer of [y]our [p]ersonal [d]ata will take place . . . unless there are adequate controls in place including the security of [y]our data and other personal information." Id.

Capiau provided Ascendum his PII "[a]s a condition of his employment." (Doc. No. 1 ¶

47). He alleges that Ascendum "required [him] to provide that PII in order to obtain employment and payment for that employment." (Id.). When Capiau provided Ascendum his PII, he presumed "that a portion of the funds paid to [Ascendum] (and/or derived from [Capiau's] employment) would be used to pay for adequate cybersecurity and protection of his PII." (Id. ¶ 49).

On May 27, 2023—during Capiau's term of employment—Ascendum suffered a data breach. On June 19, 2023, a cybercrime group known as "ALPHV Blackcat" ("Blackcat") took credit for the data breach and issued a ransom demand. See BlackCat/ALPHV Ransomware Victim: Ascendum Machinery, REDPACKET SECURITY (June 21, 2023) https://www.redpacketsecurity.com/alphv-ransomware-victim-ascendum-machinery/. Blackcat is a ransomware group recognized as a threat by the Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, and Department of Health and Human Services. See *#StopRansomware: ALPHV Blackcat*, CISA (Feb. 27, 2024) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a. Less than a month after issuing its ransom demand, Blackcat claimed to have published the stolen data—including current and former employees' PII—on the dark web. (Doc. No. 1 ¶ 40). Cybercriminals use the dark web to sell stolen data. Brenda R. Sharton, Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?, HARV. BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-forsale-on-the-dark-web-should-you-buy-it-back.

On September 1, 2023, Ascendum realized that the Blackcat breach had compromised current and former employees' PII. The compromised PII includes names, social security numbers, dates of birth, physical addresses, utility and telephone bills, government ID information, and copies of police reports. (Doc. No. 1 Ex. A). The breach also compromised the PII of some employees' minor children. (Id.) Ascendum notified victims—now putative class members—of

the breach on January 18, 2024, 236 days after the May 27, 2023, hack. Ascendum's January 2024 Notice of Data Breach ("Notice") acknowledged that the breach put victims at an increased risk of identity theft and fraud. (Doc. No. 1 Ex. A). While the number of persons injured by the breach remains unknown, Capiau avers that "upon information and belief, the putative class has over one hundred members." (Doc. No. 1 ¶ 29).

Capiau provided Ascendum his PII before the May 2023 hack. He alleges that his PII was compromised by Blackcat and has been or will soon be published on the dark web. Since learning of the breach, Capiau has expended "significant time and effort monitoring his accounts to protect himself from identity theft," and suffered a "spike in spam calls and scam emails, text messages, and phone calls" including from persons pretending to be Ascendum's CEO. (Doc. No. 1 ¶¶ 55–56). Capiau also claims to suffer from anxiety, sleep disruption, stress, fear, and frustration due to the data breach. (Id. ¶ 58). In financial terms, Capiau claims the data breach diminished the value of his PII (which he characterizes as "intangible property") and that he "anticipates spending considerable amounts of time and money to try and mitigate his injuries." (Id. ¶¶ 60, 62). While Ascendum has offered some breach victims "credit monitoring and identity related services," Capiau maintains that "such services are wholly insufficient to compensate Plaintiff and [c]lass members." (Id. ¶ 36).

Capiau charges that Ascendum's failures to "adequately train its employees on cybersecurity" and/or "maintain reasonable security safeguards or protocols to protect the Class's PII" caused the breach by making Plaintiffs' PII a soft target for cybercriminals. (Doc. No. 1 ¶ 5). Given the recent increase in cyberattacks and consequent data breaches, Capiau contends, Ascendum should have known that their employees' PII constituted a potential target and thus taken appropriate security measures like those recommended by the Federal Trade Commission.

(Id. ¶¶ 73–82). Capiau further alleges that Ascendum's cybersecurity practices failed to meet accepted industry standards. (Id. ¶¶ 83–86).

b. Procedural Background

Based on the foregoing facts, Capiau (individually and on behalf of the putative class) brings seven causes of action against Ascendum: negligence, negligence per se, breach of implied contract, invasion of privacy, unjust enrichment, breach of fiduciary duty, and violation of the North Carolina Unfair and Deceptive Trade Practices Act ("NCUDTPA") (N.C. GEN. STAT. § 75-1.1). Capiau contends that injuries caused by the breach are redressable by a combination of injunctive relief and money damages. He also petitions the Court for a declaratory judgment clarifying Defendant's obligations with respect to his and the putative class members' PII.

Instead of answering Capiau's complaint, Ascendum responded with a Motion to Dismiss. (Doc. No. 15). Ascendum moves to dismiss Capiau's complaint under Federal Rules of Civil Procedure 12(b)(1) (lack of standing) and 12(b)(6) (failure to state a claim). Capiau responded in opposition, and Defendant replied. (Doc. Nos. 20, 21). Defendant's motion is now fully briefed and ripe for decision.

II. Legal Standard

Defendant moves to dismiss Plaintiff's complaint under FED. R. CIV. P. 12(b)(1) and 12(b)(6). Facing such motions, the Court "must draw all reasonable inferences arising from the [plaintiff's] proof, and resolve all factual disputes, in the plaintiff's favor." Mylan Labs., Inc. v. Akzo, N.V., 2 F.3d 56, 59–60 (4th Cir. 1993).

A Rule 12(b)(1) motion requires the party asserting federal subject matter jurisdiction to prove such jurisdiction is proper. In other words, a Rule 12(b)(1) motion questions whether the plaintiff "has a right to be in the district at all and whether the court has the power to hear and

dispose of [plaintiff's] claim." Holloway v. Pagan River Dockside Seafood, Inc., 669 F.3d 448, 452 (4th Cir. 2012). Plaintiff, as the party asserting jurisdiction, bears the burden to show that standing is proper on these facts. Adams v. Bain, 697 F.2d 1213, 1219 (4th Cir. 1982). The Court assesses Plaintiff's showing against the motion to dismiss standard. Overbey v. Mayor of Baltimore, 930 F.3d 215, 227 (4th Cir. 2019) (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992)).

Ruling on a motion to dismiss for lack of standing, the Court "must construe the complaint in the plaintiff's favor, accepting as true the factual allegations in the complaint." Students for Fair Admissions, Inc. v. Univ. of N.C., 1:14CV954, 2018 WL 4688388, at *2 (M.D.N.C. Sept. 29, 2018); see Deal v. Mercer Cnty. Bd. of Educ., 911 F.3d 183, 187 (4th Cir. 2018) (quoting S. Walk at Broadlands Homeowner's Ass'n, Inc. v. OpenBand at Broadlands, LLC, 713 F.3d 175, 181–82 (4th Cir. 2013)). A district court should only grant a Rule 12(b)(1) motion to dismiss "if the material jurisdictional facts are not in dispute and the moving party is entitled to prevail as a matter of law." Richmond, Fredericksburg, & Potomac R. Co. v. United States, 945 F.2d 765, 768 (4th Cir. 1991). To determine whether subject matter jurisdiction is proper, the Court may consider evidence beyond the pleadings. Evans v. B.F. Perkins Co., 166 F.3d 642, 647 (4th Cir. 1999).

A Rule 12(b)(6) motion tests whether the plaintiff "has stated a cognizable claim" and thereby challenges the "sufficiency of the complaint." Holloway, 669 F.3d at 452. In reviewing a motion to dismiss pursuant to FED. R. CIV. P. 12(b)(6), the Court must accept as true all factual allegations in the Complaint and draw all reasonable inferences in the light most favorable to the plaintiff. See Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555–56 (2007). However, to survive a Rule 12(b)(6) motion, "[f]actual allegations must be enough to raise a right to relief above the speculative level," with the complaint having "enough facts to state a claim to relief that is

plausible on its face." Id. at 570. "[T]he tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions," and "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements" are insufficient. Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (citing Twombly, 550 U.S. at 555). A complaint may survive a motion to dismiss only if it "states a plausible claim for relief" that "permit[s] the court to infer more than the mere possibility of misconduct" based upon "its judicial experience and common sense." Id. at 679 (citations omitted).

III. Discussion

a. Defendant's 12(b)(1) Motion to Dismiss for Lack of Standing

"To state a case or controversy under Article III, a plaintiff must establish standing." Spokeo, Inc. v. Robins, 578 U.S. 330, 338 (2016) (quoting Arizona Christian Sch. Tuition Org. v. Winn, 563 U.S. 125, 133 (2011)). To establish standing, a plaintiff must in turn satisfy three elements: injury, causation, and redressability. Lujan, 504 at 560–601. Moreover, Plaintiff must establish standing for each claim they raise and form of relief they request. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2208 (2021). Each element of the standing inquiry "must be shown 'with the manner and degree of evidence required at the successive stages of the litigation.'" Brooks v. Receivables Performance Mgmt. LLC, No. 3:21-CV-579, 2023 WL 4228984, at *2 (W.D.N.C. June 27, 2023) (quoting TransUnion, 141 S. Ct. at 2208).

Defendant's argument highlights the injury and redressability prongs of the standing inquiry. For standing purposes, "the plaintiff must have suffered an 'injury in fact'—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical." Lujan, 504 U.S. at 560. Assessing Plaintiff's alleged injury, the Court "accept[s] as valid the merits of [the plaintiff's] legal claims." See Fed. Election Comm'n v.

Cruz, 142 S. Ct. 1638, 1647 (2022); see also Warth v. Seldin, 422 U.S. 490, 500 (1975).

To satisfy the redressability prong of the inquiry, Plaintiff "must show that 'it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.'" Sierra Club v. U.S. Dep't of the Interior, 899 F.3d 260, 284 (4th Cir. 2018) (quoting Friends of the Earth, Inc. v. Laidlaw, 528 U.S. 167, 181 (2000)). Plaintiff "need not show that a favorable decision will relieve every injury." Id. (quoting Larson v. Valente, 456 U.S. 228, 243 n.15 (1982)). Instead, Plaintiff "need only show that they personally would benefit in a tangible way from the court's intervention." Id. (internal quotation marks omitted).

i. Injury in Fact: Actual Injury

A concrete Article III injury must be "real, and not abstract." TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2204 (2021). Defendant contends that Plaintiff disappoints Article III's actual injury requirement "[b]y proffering nothing but hypothetical theories of future injury." (Doc. No. 15-1 at 5). Because Plaintiff does not claim that his identity has been stolen because of the breach, Defendant argues, Plaintiff has not alleged an Article III injury and therefore lacks standing.

Defendant is correct in principle: "the mere potential compromise of personal information does not amount to a concrete harm for constitutional standing purposes." Stamat v. Grandizio Wilkins Little & Matthews, LLP, No. CV SAG-22-00747, 2022 WL 3919685, at *6 (D. Md. Aug. 31, 2022). Nor does increased risk of identity theft following a data breach, standing alone, confer standing to sue. Beck v. McDonald, 848 F.3d 262, 272 (4th Cir. 2017) (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 407 (2013)). In doctrinal terms, "a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." Hutton v. Nat'l Bd. of Examiners in Optometry, Inc., 892 F.3d 613, 621 (4th Cir. 2018); see O'Leary v. TrustedID, Inc., 60 F.4th 240, 244 (4th Cir. 2023); Holmes v. Elephant Ins. Co., No.

3:22CV487, 2023 WL 4183380, at *1 (E.D. Va. June 26, 2023). That is so because, without evidence of actual misuse, a data breach plaintiff fails to "push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." Beck, 848 F.3d at 274 (citing Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 386 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007); Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir. 2010)).

To survive Defendant's 12(b)(1) motion, then, Plaintiff must allege actual misuse of his PII disclosed by the data breach. Beck, 848 F.3d at 272. Actual misuse is the keystone of Article III injury in Fourth Circuit data breach case law. See O'Leary, 60 F.4th at 244 (comparing Hutton and Beck); In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 459 (D. Md. 2020) (same); Solomon v. ECL Grp., LLC, No. 1:22-CV-526, 2023 WL 1359662, at *3 (M.D.N.C. Jan. 31, 2023) (same); Farley v. Eye Care Leaders Holdings, LLC, No. 1:22-CV-468, 2023 WL 1353558, at *3 (M.D.N.C. Jan. 31, 2023) (same); Podroykin v. Am. Armed Forces Mut. Aid Ass'n, 634 F. Supp. 3d 265, 270 (E.D. Va. 2022); compare Bank of La. v. Marriott Int'l, Inc., 438 F. Supp. 3d 433, 440 (D. Md. 2020); McCreary v. Filters Fast LLC, No. 3:20-CV-595-FDW-DCK, 2021 WL 3044228, at *5 (W.D.N.C. July 19, 2021) (concrete injury established by plaintiffs' allegation of actual misuse) with Kimbriel v. ABB, Inc., No. 5:19-CV-215-BO, 2019 WL 4861168, at *3 (E.D.N.C. Oct. 1, 2019); Krohm v. Epic Games, Inc., 408 F. Supp. 3d 717, 720 (E.D.N.C. 2019); Stamat, 2022 WL 3919685, at *5 (no standing where plaintiffs failed to show misuse of their data as a result of underlying breach). Other circuits have adopted a similar approach. See, e.g., Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 373 (1st Cir. 2023); In re Equifax Inc. Customer Data Sec. Breach Litig., 999 F.3d 1247, 1262 (11th Cir. 2021); Attias v. CareFirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017); Green-Cooper v. Brinker Int'l, Inc., 73 F.4th

883, 889 (11th Cir. 2023), cert. denied sub nom. Brinker Int'l, Inc. v. Steinmetz, 144 S. Ct. 1457 (2024) (citing Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1343 (11th Cir. 2021)).

One way for a data breach plaintiff to establish actual misuse—and thus Article III injury—is to credibly plead "that their data [has] been used in a fraudulent manner" as a consequence of the breach. Stamat, 2022 WL 3919685, at *5 (citing Hutton, 892 F.3d at 622). Capiau alleges that, following Ascendum's data breach, he experienced an increase in spam emails, text messages, and phone calls, including some claiming to be from Ascendum's CEO. While Capiau's receipt of spam does not itself constitute Article III injury, it does show that his PII is being used in a fraudulent manner due to the Ascendum breach. Based on this credible showing of actual misuse, the Court concludes that Capiau has established a concrete and actual injury sufficient to confer Article III standing. See Solomon v. ECL Grp., LLC, No. 1:22-CV-526, 2023 WL 1359662, at *4 (M.D.N.C. Jan. 31, 2023) (citing Krakauer v. Dish Network, L.L.C., 925 F.3d 643, 653 (4th Cir. 2019); Garey v. James S. Farrin, P.C., 35 F.4th 917, 921–22 (4th Cir. 2022); McCreary, 2021 WL 3044228, at *4–5); Farley v. Eye Care Leaders Holdings, LLC, No. 1:22-CV-468, 2023 WL 1353558, at *4 (M.D.N.C. Jan. 31, 2023).

Defendant protests that increased spam is not injury in fact, citing the decisions of "[n]umerous courts" outside the Fourth Circuit. (Doc. No. 15-1 at 10). But the Court does not find that receiving spam is, itself, an injury. Instead, the Court finds that Capiau's increased receipt of spam, including from actors impersonating Ascendum's CEO, support the inference that Capiau's PII has been mis-used as a consequence of the Ascendum breach. Actual mis-use—not receipt of spam—constitutes the concrete injury upon which Capiau has standing to sue.

ii. Injury in Fact: Intangible Injury

In TransUnion, the Supreme Court held that intangible injuries are sufficiently "actual"

where they bear a "close relationship to harms traditionally recognized" as sufficient for standing in American courts, such as "reputational harms, disclosure of private information, and intrusion upon seclusion." 141 S. Ct. at 2204. The intangible harm inquiry "asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury," but "does not require an exact duplicate." Id. Here, Plaintiff raises a common law invasion of privacy claim. In Webb, the First Circuit held that allegations of actual PII misuse arising from a data breach were analogous to common law invasion of privacy, and therefore satisfied the TransUnion intangible harm inquiry. Webb, 72 F.4th at 374 (noting that a common law invasion of privacy claim "protect[s] ... the interest of the individual in the exclusive use of his own identity, in so far as it is represented by his name or likeness, and in so far as the use may be of benefit to him or to others.") (quoting Restatement (Second) of Torts § 652C cmt. a (Am. L. Inst. 1977)); see also Bohnak v. Marsh & McLennan Cos., Inc., 79 F.4th 276, 285 (2d Cir. 2023) (citing Restatement (Second) Torts § 652D) ("Similar to the publication of misleading information about some of the plaintiffs in TransUnion, the core injury here—exposure of Bohnak's private PII to unauthorized third parties—bears some relationship to a well-established common-law analog: public disclosure of private facts."). The Fourth Circuit reached a similar conclusion in Garey v. James S. Farrin, P.C., affirming that invasion of privacy "has long provided a basis for recovery at common law." 35 F.4th at 921. Based on Capiau's allegations of actual PII misuse, and his analogy to common law invasion of privacy, the Court finds Plaintiff's allegation of intangible harm sufficient to state an Article III injury.

iii. Injury in Fact: Future Injury

Even absent proof of actual misuse, a data breach plaintiff may have standing where they show that they face a "substantial risk" of PII misuse in the future. See Susan B. Anthony List v.

Driehaus (SBA List), 134 S.Ct. 2334, 2341 (2014); Attias v. Carefirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017). This makes good sense: otherwise, standing doctrine would prevent data breach victims from obtaining relief to prevent misuse of their data until after the data was misused. Taking identity theft as an example, the D.C. Circuit instructs that

> "the proper way to analyze an increased-risk-of-harm claim is to consider the ultimate alleged harm," which in this case would be identity theft, "as the concrete and particularized injury and then to determine whether the increased risk of such harm makes injury to an individual citizen sufficiently 'imminent' for standing purposes." Food & Water Watch[, Inc. v. Vilsack], 808 F.3d [905,] 915 [D.C. Cir. 2015] (quoting Public Citizen, Inc. v. Nat'l Highway Traffic Safety Admin., 489 F.3d 1279, 1298 (D.C. Cir. 2007)).

Attias, 865 F.3d at 627. Because identity theft constitutes a concrete and particularized injury, "[t]he remaining question, . . . is whether the complaint plausibly alleges that [Plaintiff] now face[s] a substantial risk of identity theft as a result of [Defendant's] alleged negligence in the data breach. (Id.).

Even absent a showing of actual misuse, Plaintiff satisfies the concreteness and imminence requirements of Article III injury by highlighting the "substantial risk" that his PII will be misused in the future. Plaintiff does so by pointing out that the Ascendum breach was the result of a targeted effort to access employees' PII. "Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints." Galaria, 663 F App'x at 388; see also Beck, 848 F.3d at 272. "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." Remijas, 794 F.3d at 693. Indeed, "one is hard pressed to think of a reason why data thieves would engage in a large-scale and sophisticated operation to steal electronic data containing personal information and only personal information other than to misuse it." Farley,

No. 1:22-CV-468, 2023 WL 1353558, at *3 (M.D.N.C. Jan. 31, 2023). Because Capiau credibly pleads that a seasoned cybercriminal group hacked into Ascendum's database to steal employees' PII, the Court draws the reasonable inference that Capiau faces a "substantial risk" of actual PII misuse in the future. Plaintiff Capiau therefore establishes a concrete, particularized, and imminent injury sufficient to confer Article III standing.

iv. Injury in Fact: Mitigation Efforts

Next, Defendant takes aim at Capiau's claim that the data breach caused him to spend "significant time and effort" monitoring his accounts to mitigate the risk of identity theft, and that such mitigation efforts constitute Article III injury. (Doc. No. 15-1 at 7 (quoting Doc. No. 1 ¶ 55)). Defendant's argument falls short. In the Fourth Circuit, a data breach plaintiff need not show a classic pocketbook injury (i.e., economic loss) to establish standing. McCreary, 2021 WL 3044228, at *4 (citing Hutton, 892 F.3d at 622). Instead, the "time and resources" a plaintiff must expend to repair their credit or otherwise detect, prevent, or mitigate identity theft or unauthorized use of their PII are sufficient to confer standing. McCreary, 2021 WL 3044228, at *6 (quoting Hutton, 892 F.3d at 622 and citing United States v. Students Challenging Regulatory Agency Procedures, 412 U.S. 669, 686 (1973)).

Where concrete injury is imminent—as it is after a plaintiff's PII is stolen in a targeted hack—a plaintiff's voluntary mitigation efforts are cognizable as Article III harms. See Stamat, No. CV SAG-22-00747, 2022 WL 3919685, at *7 (D. Md. Aug. 31, 2022); Beck, 848 F.3d at 276–77 (citing Remijas, 794 F.3d at 694; Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011)); Antman v. Uber Techs., Inc., No. 3:15cv175, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015); Clapper, 568 U.S. at 402. The Fourth Circuit, alongside several of its sisters, has held that a plaintiff's pursuit of protective measures in response to a data breach posing a substantial and

imminent risk of future harm—as the Court finds this breach does—constitutes a concrete injury sufficient to confer Article III standing. See Hutton, 892 F.3d at 622; Clemens v. ExecuPharm Inc., 48 F.4th 146, 158 (3d Cir. 2022); Galaria, 663 F. App'x at 388–89; Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016); Equifax, 999 F.3d at 1262; Webb, 72 F.4th at 377; Bohnak, 79 F.4th at 279 (citing McMorris v. Carlos Lopez & Assocs., 995 F.3d 295, 303 (2d Cir. 2021)). Because Blackcat's targeted breach of Ascendum employees' PII poses a substantial risk of imminent harm, the time and effort Capiau dedicated to mitigation efforts constitute Article III injuries.

v. Injury in Fact: Diminished Value of PII

Capiau pleads that the Ascendum breach decreased the value of his PII. Defendant responds that even if such diminution can constitute Article III injury, Capiau fails to plead facts from which the Court can infer that the value of Plaintiff's PII has diminished.

District courts in this and other circuits have recognized the "diminution in value" of a data breach victim's "personal and financial information" as an Article III harm. McCreary, No. 3:20-CV-595-FDW-DCK, 2021 WL 3044228, at *6 (W.D.N.C. July 19, 2021) (citing In re Marriott, 440 F. Supp 3d at 462–63); Stamat, No. CV SAG-22-00747, 2022 WL 3919685, at *7; see also Pruchnicki v. Envision Healthcare Corp., 439 F. Supp. 3d 1226, 1234 (D. Nev. 2020), affirmed 845 Fed. App'x 613 (9th Cir. 2021) ("Diminution in value of personal information can be a viable theory of damages."). Likewise, this Court cannot "ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy." In re Marriott, 440 F. Supp. 3d at 462.

Nevertheless, Capiau must allege facts suggesting that his PII's value did in fact decrease due to the Ascendum breach. He can do so by establishing that the data breach "interfered" with

his "fiscal autonomy" by impairing his "ability to participate in the economic marketplace," Smallman v. MGM Resorts Int'l, 638 F. Supp. 3d 1175 (D. Nev. 2022), that is, "the economic benefit [he] derives from being able to purchase goods and services remotely and without the need to pay in cash or a check." See In re Marriott Int'l, Inc., 440 F. Supp. at 462. Plaintiff's complaint is bereft of such allegations. Therefore, Plaintiff lacks standing to pursue claims predicated on the diminished value of his PII.

But Defendant's victory on this point rings hollow. None of Plaintiff's claims are predicated on PII value diminution. And, as the Court found above, the remainder of Plaintiff's alleged injuries are sufficient to confer Article III standing. Therefore, the Court's finding that Capiau lacks standing to seek relief on diminished PII value alone does not require the dismissal of any of Plaintiff's substantive legal claims.

vi. Injury in Fact: Emotional Distress

Next, Defendant argues that Plaintiff's emotional distress claims are insufficiently concrete to state an Article III injury. The Court agrees. While emotional injury can constitute actual harm sufficient to confer Article III standing, "bare assertions of emotional injury" will not do. TransUnion, 141 S. Ct. at 2211 n.7; Beck, 848 F.3d at 273 (citing Doe v. Chao, 540 U.S. 614, 624–25 (2004)). Fear of identity theft, fraud, or generalized "emotional upset" caused by news of a data breach are thus insufficient to state an Article III injury. Beck, 848 F.3d at 272; see also Stamat, 2022 WL 3919685, at *6; Baysal v. Midvale Indem. Co., 78 F.4th 976, 977 (7th Cir. 2023). Capiau's generalized allegations that the data breach caused him to suffer "anxiety, sleep disruption, stress, fear, and frustration" are not concrete enough for Article III standing. Nor can Capiau attempt to analogize his alleged emotional distress injury to intentional infliction of emotional distress. See TransUnion, 141 S. Ct. at 2211 n.7. Thus, Plaintiff's threadbare emotional

distress claim is insufficient to confer Article III standing.

As with Defendant's success with respect to PII value diminution, though, this victory rings hollow. None of Plaintiff's claims rely exclusively on an emotional distress injury. Therefore, Capiau's lack of standing to recover on emotional damages does not require dismissing any of his substantive legal claims.

vii. Causation (Traceability)

While Defendant's 12(b)(1) motion does not appear to challenge the causation element of the Article III standing inquiry, the Court addresses it here for the sake of completeness. "[T]he 'case or controversy' limitation of Art[icle] III still requires that a federal court act only to redress injury that fairly can be traced to the challenged action of the defendant, and not injury that results from the independent action of some third party not before the court." Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 41–42 (1976); see Lujan, 504 U.S. at 560. The Article III traceability inquiry is not as strict as the tort causation standard, demanding only that the data breach plausibly caused Plaintiff's injury. Solomon v. ECL Grp., LLC, No. 1:22-CV-526, 2023 WL 1359662, at *4 (M.D.N.C. Jan. 31, 2023) (citing Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 161 (4th Cir. 2000); Bank of La. v. Marriott Int'l, Inc., 438 F. Supp. 3d 433, 441 (D. Md. 2020)). Thus, Plaintiff need only establish "a genuine nexus" between his injury and Defendant's alleged conduct. Gaston Copper Recycling Corp., 204 F.3d at 161. Fourth Circuit courts have routine found traceability in the data breach context where plaintiffs provided defendants with PII and those defendants subsequently fell victim to a targeted data breach resulting in the disclosure and misuse of plaintiff's PII. See, e.g., Hutton, 892 F.3d at 622; McCreary, No. 3:20-CV-595-FDW-DCK, 2021 WL 3044228, at *5 (W.D.N.C. July 19, 2021); In re Marriott, 440 F. Supp. 3d at 467. That is precisely what Capiau claims happened here. Thus, Capiau's alleged injuries are

fairly traceable to Defendant's conduct.

viii. Redressability

In addition to money damages, Capiau seeks declaratory and injunctive relief, specifically an order requiring Defendant to "use adequate security consistent with industry standards to protect the data entrusted to it." (Doc. No. 1 ¶ 191). Defendant submits that, because Capiau fails to plead an injury that would be redressed by such an injunction, he lacks standing to pursue claims for equitable relief. (Doc. No. 15-1 at 11). The Court agrees.

Here, Capiau seeks three forms of relief: money damages, injunction, and a declaratory judgment. Defendant's redressability challenge takes aim at the latter two forms of relief, based on the apparent assumption that a declaratory judgment is an equitable remedy. Defendant's assumption is incorrect—declaratory judgment is a statutory remedy, not an equitable one, see 28 U.S.C § 2201(a)—but the basic analysis remains the same: Capiau "must 'demonstrate standing separately for each form of relief sought.'" TransUnion LLC, 141 S. Ct. at 2210 (quoting Friends of the Earth, Inc., 528 U.S. at 185). In simple terms, he must show that money damages, injunctive relief, and a declaratory judgment will redress the harms visited upon him by Defendant's alleged misdeeds.

Capiau has standing to pursue money damages. The Court found above that Capiau credibly alleges multiple injuries in fact traceable to Defendant's conduct. Where a plaintiff has suffered an injury in fact, damages will typically be available. Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 828 (7th Cir. 2018). Thus, where a plaintiff satisfies Article III's standing requirements, that plaintiff has "almost certainly sustained cognizable damages." Allen v. Wenco Mgmt., LLC, No. 1:23 CV 103, 2023 WL 6456571, at *3 (N.D. Ohio Sept. 29, 2023). Because Capiau suffered multiple injuries in fact, the Court concludes that he has standing to pursue money

damages to redress those alleged injuries.

As to equitable relief, however, the Court finds that Capiau fails to satisfy the redressability inquiry and therefore lacks standing. To pursue injunctive relief, Capiau must establish that, absent injunctive relief, he is "likely to suffer future injury," City of Los Angeles v. Lyons, 461 U.S. 95, 105 (1983), and that the requested injunction would mitigate the future injury Capiau is likely to suffer. See Lujan, 504 U.S. at 568–71. While Capiau has established that he is substantially likely to suffer future injury (i.e., further misuse of his PII), he cannot establish that an injunction against Ascendum would redress that injury.

"[A] person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." TransUnion, 141 S. Ct. at 2211 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013)). Put another way, "a material risk of future harm can satisfy the concrete harm requirement," "but only as to injunctive relief, not damages." Id. at 2210; Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 372 (1st Cir. 2023). "To have standing to pursue damages based on a risk of future harm, plaintiffs must demonstrate a separate concrete harm 'caused by their exposure to the risk itself.'" Webb, 72 F.4th at 372 (quoting TransUnion, 141 S. Ct. at 2211). Where a Plaintiff's PII is compromised in a targeted attack, it stands to reason that the data is likely to be misused. Anderson v. Hannaford Bros. Co., 659 F.3d 151, 164 (1st Cir. 2011); see also McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 302 (2d Cir. 2021); Clemens, 48 F.4th at 153–54; Galaria, 663 F. App'x at 388; Remijas, 794 F.3d at 693; In re Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1029 n.13 (9th Cir. 2018); In re: U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 58–59 (D.C. Cir. 2019) ("OPM"). So too where some portion of the compromised dataset has already been misused, Anderson, 659 F.3d at 164;

McMorris, 995 F.3d at 301–02; Remijas, 794 F.3d at 693–94; In re Zappos.com, 888 F.3d at 1027 n.7; OPM, 928 F.3d at 58–59, or the data exposed is sensitive such that it presents a heightened risk of identity theft or fraud, McMorris, 995 F.3d at 302; Clemens, 48 F.4th at 154; OPM, 928 F.3d at 49, 59; Attias, 865 F.3d at 628.

Here, Plaintiff requests "injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it." (Doc. No. 1 ¶ 191). Absent an injunction, Capiau argues, he will likely suffer future injury in the event of a second data breach. (Id. ¶ 192). But that is not enough for Article III standing. Instead, Capiau must establish that a future breach is likely to occur—put another way, that Defendant's prior breach makes a second breach more likely. But Plaintiff admits that following the data breach, Defendant committed to "implement additional safeguards and review policies and procedures relating to data privacy and security." (Doc. No. 1 Ex. A). Plaintiff dismisses Defendant's efforts as "too little too late," contending that "these measures—which Defendant now recognizes as necessary—should have been implemented before the Data Breach." (Id. ¶ 33) (emphasis in the original). Maybe so. But even assuming that Defendant should have adopted additional data safeguards prior to the breach, Plaintiff fails to show—now that Defendant has adopted those safeguards—that Plaintiff remains likely to suffer future injury caused by a second breach. Because Plaintiff cannot show that Defendant's past (alleged) failures make Plaintiff more likely to suffer future injury, Plaintiff lacks standing to pursue injunctive relief requiring Defendant to adopt further data security measures. See McCreary, No. 3:20-CV-595-FDW-DCK, 2021 WL 3044228, at *7 (W.D.N.C. July 19, 2021); compare Webb, 72 F.4th at 378 (finding plaintiffs' proposed inference that a prior breach makes a future breach more likely undercut by plaintiffs' admission that defendant implemented new safeguards following the first breach) with Solomon v. ECL Grp., LLC, No. 1:22-CV-526, 2023

WL 1359662, at *4 (M.D.N.C. Jan. 31, 2023) (finding substantial risk of future data breach where defendant did not employ reasonable security measures after the first breach).

As to Capiau's request for a declaratory judgment, the Court first notes that any such judgment would likely be enforceable only through the type of injunction this Court has already found Capiau lacks standing to pursue. And even if the Court were to issue the kind of declaratory judgment Plaintiff requests, clarifying Defendant's obligations with respect to Plaintiff's PII, that judgment would not redress the injuries Plaintiff has or will suffer for the same reasons that Plaintiff's proposed injunction fails the redressability inquiry. See Miller v. Brown, 462 F.3d 312, 316 (4th Cir. 2006) (citing Lujan, 504 U.S. at 560–61). This is simply not a case where the controversy between the parties warrants issuance of a declaratory judgment. Volvo Constr. Equip. N. Am., Inc. v. CLM Equip. Co., 386 F.3d 581, 592 (4th Cir. 2004)

The Court therefore finds that, while this matter constitutes "a case of actual controversy within [the Court's] jurisdiction," Plaintiff's claims cannot be redressed by a declaratory judgment. Plaintiff therefore lacks standing to pursue a declaratory judgment in this matter.

b. Defendant's 12(b)(6) Motion to Dismiss for Failure to State a Claim

Defendant notes that Plaintiff's Complaint "potentially implicates the laws of two jurisdictions: (1) Tennessee, where Plaintiff resides, and (2) North Carolina, where Ascendum has its principal place of business." (Doc. No. 15-1 at 12). Without prejudice to a future choice of law decision—which is best deferred to the post-discovery phase, Movement Mortg., LLC v. McDonald, No. 17-716, 2018 WL 6733953, at *3 (W.D.N.C. Nov. 6, 2018); Farley, 2023 U.S. Dist. LEXIS 15480, at *14—the Court will adjudicate Defendant's 12(b)(6) motion under North Carolina law.

As Plaintiff explains, a district court must apply the choice-of-law rules of the state in

which it sits. Lamie v. Lendingtree, LLC, No. 3:22-cv-00307, 2023 U.S. Dist. LEXIS 21841, at *4 (W.D.N.C. Feb. 9, 2023) (citing Colgan Air, Inc. v. Raytheon Aircraft Co., 507 F.3d 270, 275 (4th Cir. 2007)). This Court sits in North Carolina, which uses the lex loci delicti choice of law principle, requiring courts to apply the law of "the state where the last act occurred giving rise to the injury." Id. (quoting Harco Nat'l Ins. Co. v. Grant Thornton LLP, 698 S.E.2d 719, 724 (N.C. Ct. App. 2010)). Here, the last act giving rise to Plaintiff's alleged injuries occurred in North Carolina, where Ascendum is headquartered and where the data breach transpired. See Lamie, No. 3:22-cv-00307, 2023 U.S. Dist. LEXIS 21841, at *4 (W.D.N.C. Feb. 9, 2023); Farley, 2023 U.S. Dist. LEXIS 15480, at *13. The Court will therefore analyze Plaintiff's claims under North Carolina law.

i. Negligence

To state a negligence claim in North Carolina, Plaintiff must allege that Defendant (1) owed Plaintiff a duty; (2) breached that duty; (3) such breach caused Plaintiff injury; and (4) that Plaintiff suffered damages as a result. Parker v. Town of Erwin, 776 S.E.2d 710, 729–30 (N.C. Ct. App. 2015). Defendant contends Plaintiff's negligence claim fails because Plaintiff fails to allege damages cognizable under North Carolina law. Specifically, Defendant argues that the damages Plaintiff does allege are "entirely speculative" and therefore insufficient to support a negligence claim. (Doc. No. 15-1 at 13) (citing McAdoo v. Univ. of North Carolina at Chapel Hill, 736 S.E.2d 50, 65 (N.C. Ct. App. 2013)). Not so. As discussed in the above standing analysis, Plaintiff alleges damages stemming from: (2) actual mis-use of their PII; (2) an intangible harm fairly analogous to common law invasion of privacy; (3) the substantial risk that Plaintiff's PII will continue to be mis-used in the future; and (4) opportunity and other costs imposed by reasonable mitigation efforts intended to address the substantial risk of PII mis-use. Plaintiff's factual allegations of

damages caused by Defendant's data breach are sufficient to survive Defendant's 12(b)(6) motion, and so Defendant's motion as to Plaintiff's negligence claim will be denied.

ii. Negligence Per Se

Next, Defendant moves to dismiss Plaintiff's negligence per se claim. Defendant first argues that Plaintiff cannot recover for negligence per se because Plaintiff fails to plead facts showing that he suffered cognizable damages chargeable to Defendant's negligence. That argument fails for the same reasons discussed in the foregoing section. In the alternative, Defendant contends that Plaintiff's negligence per se theory claim fails because the statute Plaintiff alleges Defendant violated—Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45—does not provide a private right of action. (Doc. No. 15-1 at 15).

Defendant misapprehends hornbook tort law. Negligence is a common law tort claim. Plaintiff does not need a cause of action under the FTC Act to sue for negligence because negligence is itself the cause of action. The elements of a negligence claim are duty, breach, causation, and damages. On a "garden variety" negligence claim, the duty element is defined by the "ordinary care" standard. Negligence per se, however, is a unique subspecies of negligence. To bring a claim of negligence per se, the plaintiff must allege that the defendant violated a statute, and that violation of the statute caused the plaintiff to suffer damages. With respect to the duty element, "[t]he common law rule of ordinary care does not apply—" instead, "the statute prescribes the standard" of care. Parker v. Colson, 266 N.C. App. 182, 186 (2019) (quoting Carr v. Murrows Transfer, Inc., 262 N.C. 550, 554 (1964)). Contrary to Defendant's apparent misunderstanding, Plaintiff does not sue for negligence per se under the FTC Act, but instead argues that the Act provides the standard of care against which Plaintiff's negligence per se claim should be assessed.

In North Carolina, a plaintiff establishes negligence per se where they show that the

defendant violated a "public safety statute," the plaintiff was a member of the class intended to be protected by the statute, and the plaintiff suffered harm due to defendant's violation thereof. Byers v. Standard Concrete Prods. Co., 268 N.C. 518, 521 (1966); Stein v. Asheville City Bd. of Educ., 360 N.C. 321, 326 (2006); Baldwin v. GTE South, Inc., 335 N.C. 544, 546 (1994); Parker, 266 N.C. App. at 186. A "public safety statute" is defined as one "impos[ing] upon [the defendant] a specific duty for the protection of others." Stein, 360 N.C. at 326 (quoting Lutz Indus., Inc. v. Dixie Home Stores, 242 N.C. 332, 341 (1955)). The FTC Act does just that, imposing upon regulated businesses a duty to avoid "unfair or deceptive acts or practices in commerce." And while it is a closer call, the Court finds that Plaintiff is a member of the class (individuals engaged in commerce) the FTC Act exists to protect—when an employee exchanges their labor and PII for employment compensation, they are undoubtedly engaged in commerce and therefore protected by the FTC Act. Whether Defendant's data security measures and related representations amount to an "unfair or deceptive" act or practice remains to be seen.

Because Plaintiff does not require a private right of action under the FTC Act to sue for negligence per se, Defendant's motion to dismiss Plaintiff's negligence per se claim will be denied.

iii. Breach of Implied Contract

Defendant next contends that Plaintiff's breach of implied contract claim should be dismissed because Plaintiff fails to allege facts showing that Defendant had a contractual obligation to protect Plaintiff's PII. Defendant's argument, premised on a formalistic and high-handed theory of classical contract, is unpersuasive.

To survive Defendant's 12(b)(6) motion as to breach of contract, Plaintiff need show only that (1) a valid contracted existed between the parties, and (2) Defendant breached the terms of that contract. Supplee v. Miller-Motte Bus. Coll., Inc., 239 N.C. App. 208, 216 (2015). Even

Defendant recognizes that a contract can arise absent explicit written agreement where an obligation is implied or presumed from the parties' acts. Snyder v. Freeman, 300 N.C. 204, 217 (1980). Here, Plaintiff entered into an employment agreement with Defendant. As a condition of Plaintiff's employment, Defendant required Plaintiff to provide to Defendant his PII. The requirement that Plaintiff provide Defendant his PII vested in Defendant an implicit obligation to adequately safeguard Plaintiffs' PII. See McKenzie v. Allconnect, Inc., 369 F. Supp. 3d 810, 821 (E.D. Ky. 2019). These allegations are "sufficient at the pleading stage for [Plaintiff's] implied contract claim to survive." Id. The Allconnect Court's analysis does not stand alone—indeed, numerous federal courts "have recognized implied-in-fact contract claims in data breach cases." In re Arby's Rest. Grp. Inc. Litig., No. 1:17-cv-0514-AT, 2018 WL 2128441, at *16 (N.D. Ga. Mar. 5, 2018); see Anderson, 659 F.3d at 158–59; Savidge v. Pharm-Save, Inc., No. 3:17-cv-186-TBR, 2017 WL 5986972, at *9 (W.D. Ky. Dec. 1, 2017); Castillo, No. 16-cv-01958-RS, 2016 WL 9280242, at *8–9 (N.D. Cal. Sept. 14, 2016)). In fact, other circuits have found implied contracts to protect PII in the merchant/customer context, a far more attenuated relationship than the employer/employee connection alleged here. See Anderson, 659 F.3d at 159 (stating that "a jury could reasonably find an implied contract between Hannaford and its customers that Hannaford would . . . . take reasonable measures to protect the information").

Even absent their employer-employee relationship, Plaintiff's provision of PII to Defendant arguably created an implicit obligation on behalf of Defendant to protect Plaintiff's PII. See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d at 463. "[I]t is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently." Castillo v. Seagate Tech., LLC, No. 16-CV-01958-

RS, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016) (citing In re Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1176 (D. Minn. 2014)).

Plaintiff sufficiently alleges that Defendant violated an implied obligation to safeguard Plaintiff's PII. See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d at 463–64 (citing Carlsen v. GameStop, Inc., 833 F.3d 903 (8th Cir. 2016); In re Yahoo! Inc. Customer Data Sec. Breach Litigation, 313 F. Supp. 3d 1113, 1130 (N.D. Cal. 2018); In re Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016); In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1224 (N.D.Cal. 2014)). Here, as in Marriott, Carlsen, Yahoo!, and Anthem, Plaintiffs show that (1) there was an implicit contract for data security based on Defendant's privacy statements, (2) Plaintiff placed significant value on data security, and (3) knowledge of Defendant's actual data security practices would have caused Plaintiff to reconsider or renege on their bargain. Id. at 465–66.

Finally, Plaintiff convincingly argues that, even assuming Defendant did not make an implied promise to protect Plaintiff's PII, Defendants surely violated their explicit commitment to "take all steps reasonably necessary to ensure that [Plaintiff's] data is treated securely." (Doc. No. 1 ¶¶ 17–18). This commitment—found in Defendant's privacy policy—arguably initiated an implied in fact contract between the parties. "A privacy policy may give rise to an implied in fact contract if it contains an exchange of promises and consideration above and beyond the offeror's existing legal duties." Allen v. Novant Health, Inc., No. 1:22-CV-697, 2023 WL 5486240, at *3 (M.D.N.C. Aug. 24, 2023) (citing J.R. v. Walgreens Boots All., Inc., No. 20-1767, 2021 WL 4859603, at *6 (4th Cir. 2021) (per curiam) (unpublished)). True, where a plaintiff is "unaware" of defendant's use of plaintiff's PII, "there is no basis to conclude that they entered into an implied contract . . . that included a term restricting its use." J.R., No. 20-1767, 2021 WL 4859603, at *5

(4th Cir. 2021) (per curiam) (unpublished). Here, though, Plaintiff plausibly alleges that he was aware that Defendant required and intended to use his PII. Thus, the Fourth Circuit's rationale for affirming dismissal of the implied contract claim in J.R. does not control this case. Because it remains unclear whether the privacy policy in question "merely contains information" as opposed to an exchange of promises and consideration, J.R., 2021 WL 4859603, at *6 (quoting In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 610–11 (9th Cir. 2020)); see also Brush v. Miami Beach Healthcare Grp. Ltd., 238 F. Supp. 3d 1359, 1367 (S.D. Fla. 2017), the Court grounds its decision to deny Defendant's 12(b)(6) motion as to Plaintiff's contract claim on the employer/employee family of cases analyzed above. See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d at 463; McKenzie, 369 F. Supp. 3d at 821; Castillo, No. 16-CV-01958-RS, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016).

iv. Invasion of Privacy

As to Plaintiff's invasion of privacy (intrusion upon seclusion) claim, Defendant contends that Plaintiff failed to allege—as they must—that Defendant intentionally intruded upon Plaintiff's solitude or seclusion. Defendant is correct on the law: absent a showing of intent, or facts from which Defendant's intent can be inferred, Plaintiff's invasion of privacy claim must be dismissed.

In North Carolina, intrusion upon seclusion is an intentional tort. To prevail on such a claim, Plaintiff must show that Defendant "intentionally intrude[d], physically or otherwise, upon the solitude or seclusion of [Plaintiffs] or [their] private affairs or concerns." Smith v. Jack Eckerd Corp., 101 N.C. App. 566, 568 (1991) (quoting Restatement (Second) of Torts § 652B). Defendant's intent is therefore an essential element of Plaintiff's invasion of privacy claim. See Miller v. Brooks, 123 N.C. App. 20, 26–27 (1996); Toomer v. Garrett, 155 N.C. App. 462, 479 (2002); Tillet v. Onslow Mem'l Hosp., Inc., 715 S.E.2d 538, 540 (N.C. Ct. App. 2011). Plaintiff

responds that Defendant "intentionally" intruded upon Plaintiff's seclusion because Defendant "knew its inadequate cybersecurity practices would cause injury to Plaintiff and the Class." (Doc. No. 1 ¶¶ 150–53). This allegation is sufficient to save Plaintiff's invasion of privacy claim from 12(b)(6) dismissal. In North Carolina, an employer acts with "intent" to cause a result (here, intrusion upon seclusion) where they intentionally engage in misconduct (here, fail to protect Plaintiffs' PII) despite knowing it is substantially certain to seriously injure employees. Shaw v. Goodyear Tire & Rubber Co., 225 N.C. App. 90, 98–99 (2013). Thus, to prevail on their invasion of privacy claim, Plaintiff must show that Defendant knew that its lackluster cybersecurity approach was substantially certain to result in Plaintiff's PII being exposed. That will be a tall order. Nevertheless, Plaintiff's allegations survive Defendant's motion to dismiss.

v. Unjust Enrichment

Next, Defendant moves to dismiss Plaintiff's unjust enrichment claim, arguing that Plaintiff did not confer upon Defendant a "monetary benefit" in the form of his PII. In light of recent persuasive authority from district courts within and without this circuit, Defendant's argument falls short.

To prevail on their unjust enrichment claim, a plaintiff must show that "(1) benefits [were] conferred on defendant by plaintiff; (2) appreciation of such benefits by defendant; and (3) acceptance and retention of such benefits under such circumstances that it would be inequitable for defendant to retain the benefit without payment of value." Lake Toxaway Cmty. Ass'n, Inc. v. RYF Enter., LLC, 742 S.E.2d 555, 561 (N.C. Ct. App. 2013). Defendant attacks the first and third elements, contending that Defendant did not "benefit" from Plaintiff's conferral of PII. (Doc. No. 15-1 at 19) (quoting In re Arthur J. Gallagher Data Breach Litig., No. 22-137, 2022 WL 4535092, at *10 (N.D. Ill. Sept. 28, 2022)). But an unjust enrichment claim can lie even where the benefit

conferred is not monetary. And Defendant cannot be heard to argue that Defendant was indifferent to Plaintiff's provision of PII, since such provision was a condition of Plaintiff's employment.

Here, Defendant allegedly accepted the benefits accompanying Plaintiff's data without implementing adequate safeguards to protect Plaintiff's PII. Defendant thus retained Plaintiff's data, and accompanying benefit, at Plaintiff's expense. See In re Capital One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 413 (E.D. Va. 2020); see also In re Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 U.S. Dist. LEXIS 70594, at *174–75 (N.D. Cal. May 27, 2016) (same). That is sufficient for Plaintiffs' unjust enrichment claim to survive Defendant's 12(b)(6) motion.

vi. Breach of Fiduciary Duty

Sixth, Defendant moves to dismiss Plaintiff's breach of fiduciary duty claim, asserting that Plaintiff's complaint fails to allege facts establishing that Defendant was Plaintiff's fiduciary.

A fiduciary relationship is a necessary element of a North Carolina breach of fiduciary duty claim. French Broad Place, LLC v. Asheville Sav. Bank, S.S.B., 259 N.C. App. 769, 787 (2018). Such relationship exists "wherever confidence on one side results in superiority and influence on the other side; where a special confidence is reposed in one who in equity and good conscience is bound to act in good faith and with due regard to the interests of the one reposing the confidence." White v. Consol. Planning, Inc., 603 S.E.2d 147, 155 (N.C. Ct. App. 2004). The relationship between employer and employee is generally not a fiduciary relationship. See Dalton v. Camp, 353 N.C. 647, 651 (2001); Curry v. Schletter Inc., No. 17-0001, 2018 WL 1472485, at *5 (W.D.N.C. Mar. 26, 2018). Plaintiff contends that his relationship to Defendant is different, however, because Defendant made receipt of Plaintiff's PII a condition of his employment. (Doc. No. 1 ¶ 170). Given that most employers collect employees' PII, Plaintiff's proposed exception to

Dalton would swallow the rule. For that reason, the Court finds that Plaintiff failed to plead facts from which a fiduciary relationship can be inferred. Defendant's motion to dismiss Plaintiff's breach of fiduciary duty claim will, therefore, be granted.

vii. Violation of NCUDTPA

Finally, Defendant moves to dismiss Plaintiff's NCUDTPA claim, contending that Plaintiff's complaint fails to (1) satisfy the heightened pleading requirements applicable to fraud claims under FED. R. CIV. P. 9(b), and (2) allege actual injury. The Court rejects Defendant's second objection to Plaintiff's NCUDTPA claim for reasons articulated in the foregoing standing analysis: Plaintiff alleges facts that, if true, support a finding of actual injury.

As to Defendant's Rule 9(b) objection, Plaintiff responds that his NCUDTPA claim does not sound in fraud, but instead targets Defendant's allegedly unfair business practices. Plaintiff is correct that Rule 9(b) does not apply to NCUDTPA claims that do not sound in fraud. See Burn v. Lend Lease (US) Pub. P'ships LLC, No. 7:20-CV-174-D, 2021 U.S. Dist. LEXIS 172963, at *21 (E.D.N.C. Sep. 13, 2021); Gress v. Rowboat Co., 190 N.C. App. 773, 776, 661 S.E.2d 278, 281 (2008) ("[I]t is not necessary for the plaintiff to show fraud [under UDTPA.]"); In re Equifax I, 362 F. Supp. at 1335–36; Perdue v. Hy-Vee, Inc., 455 F. Supp. 3d 749, 769 (C.D. Ill. 2020). To the extent that Plaintiff's NCUDTPA claim pertains to Defendant's allegedly unfair business practices—i.e., Defendant's failure to implement and maintain adequate cybersecurity measures and to warn Plaintiff of the breach—Defendant's motion will be denied.

IV. Conclusion

For the foregoing reasons, the Court will grant in part and deny in part Defendant's motion to dismiss. Specifically, the Court will grant Defendant's Rule 12(b)(1) motion as to Plaintiff's alleged injuries of diminished PII value and emotional distress, and requests for declaratory and

injunctive relief. The Court will likewise grant Defendant's Rule 12(b)(6) motion as to Plaintiff's breach of fiduciary duty claim. In all other respects, Defendant's motion to dismiss will be denied.

ORDER

IT IS, THEREFORE, ORDERED that Defendant's motion to dismiss (Doc. No. 15) is **GRANTED** in part and **DENIED** in part. Plaintiff's requests for declaratory and injunctive relief, and Plaintiff's effort to recover based on diminution in the value of Plaintiff's PII and emotional distress, are hereby **DISMISSED**. Plaintiff's breach of fiduciary duty claim is likewise **DISMISSED**. In all other respects, Defendant's motion is **DENIED**.

SO ORDERED.

Signed: August 8, 2024